Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.570 – 573

RESEARCH ARTICLE

Binary Visual Cryptography Scheme for Cheating Prevention

Sanket Chaurasia, Shreeti Sinha, Kanchan Jaybhay, Suresh Bhuj

Computer Department, Dr. D. Y. Patil Institute of Engineering and Technology, Pimpri, India

get2sankett@gmail.com; mahisinha42@gmail.com; kanchanjaybhay7@gmail.com; sureshbhuj@gmail.com

Abstract— ***Visual cryptography, is a scheme that divides a secret image into several shares, Many researches about visual secret sharing and its applications have been recently proposed. Unfortunately, the cheating attack in which evil participants cheat the honest one(s) by making a fake share image has come into existence. Some cheating prevention measures have been proposed but was all in vain as it resulted in rise of disadvantages such as :***

(1) maintaining extra share images used to verify the integrity of a share image,

(2) pixel expansion,

(3) increase in cost and

(4) giving equivocal or unclear cheating detection.

In this paper, we have mentioned some schemes like hiding of secret image into those shares along with verification code which will be hidden from all the participants to overcome the above mentioned disadvantages.

Introduction—With the increase in computer technology and the development of networks, the transmission of images becomes a daily operation. For the security of secret images cryptosystems such as DES, and AES have been proposed. But both are expensive.

Visual secret sharing (VSS), first proposed by Naor and Shamir in 1995, encodes a secret image to create several shares which is distributed among the participants. Participants decodes the secret by stacking the collected shares to reconstruct the secret image. A k-out-of-n (k,n) visual secret sharing scheme means a secret image is encoded into n shares, and stacking of k or more shares can reconstruct the secret image. In VSS scheme, a secret image is divided into two share images SA and SB by a code-book . According to the the color of a pixel of secret images, SA and SB are assigned a sub-block for secret information. The size of sub-blocks is such that the size of the share images and reconstructed image is in expanded form. In the VSS environment, cheating occurs when some evil participants, tries to cheat honest participant .In 2006, Horng et al said that the (k,n) VSS exists the cheating problem if k < n. Eg: Participants A and B may cheat the honest participant C by giving a fake share image.

Let as assume that Participants A and B obtain sub-pixel respectively. The participants A and B can conclude that the sub-pixel of participant C is according to the codebook. By using the VSS, participants A and B can do nothing if they hope the stacked result with participant C is white/black, Therefore, the cheating problem does exist in (k,n) VSS if k < n .

I. Introduction

Many papers have proposed to solve the cheating problem.

1)Yang and Laih proposed two approaches to detect the fake shares.

- It needs the help of a trusted authority (TA). TA holds a check share. If stacking the check share with the share of a participant, the verification image can be reconstructed to differentiate the participant.
- The second approach is a kind of (k,n) VSS scheme. Any two of them can reveal the verification image used to verify the validity of a share image, while at least k shares can reconstruct the secret image.

2)Horng et al. proposed two schemes to prevent VSS from cheating.

- Every participant has two share images. The generic share image and the verification share image
- Adopt a (2,n + e) VSS scheme in which the dealer generates n + e shares but deliver n share images to n participants while l shares are discarded.

Unfortunately, the unclear stacked result cannot tell participants if the cheating does happen.

3)Hu and Tzeng proposed three cheating methods and a preventive scheme.

- The first and second cheating methods aim at the general VSS scheme in which the shares made which is of no use.
- The third cheating method attacks the extensional VSS scheme where the shares are meaningful.

This paper proposes a new scheme by combining two VSS schemes in one. It adopts the hybrid codebooks which are skillfully designed to achieve the goal that any two shares can be used to reconstruct two secret images, i.e., the verification and the original secret images. But the difficulty was that how to design the hybrid codebook. With reconstructed unambiguous verification images, the validity of shares can be authenticated so that the proposed scheme can detect fake shares. It removes all the disadvantages existing in the related works.

1) The verification images are designed to hide in the share images.
2) The computation cost in encoding is low.

Finally, once the cheating attack happens, the proposed scheme gives an unclear result of reconstructed secret image.

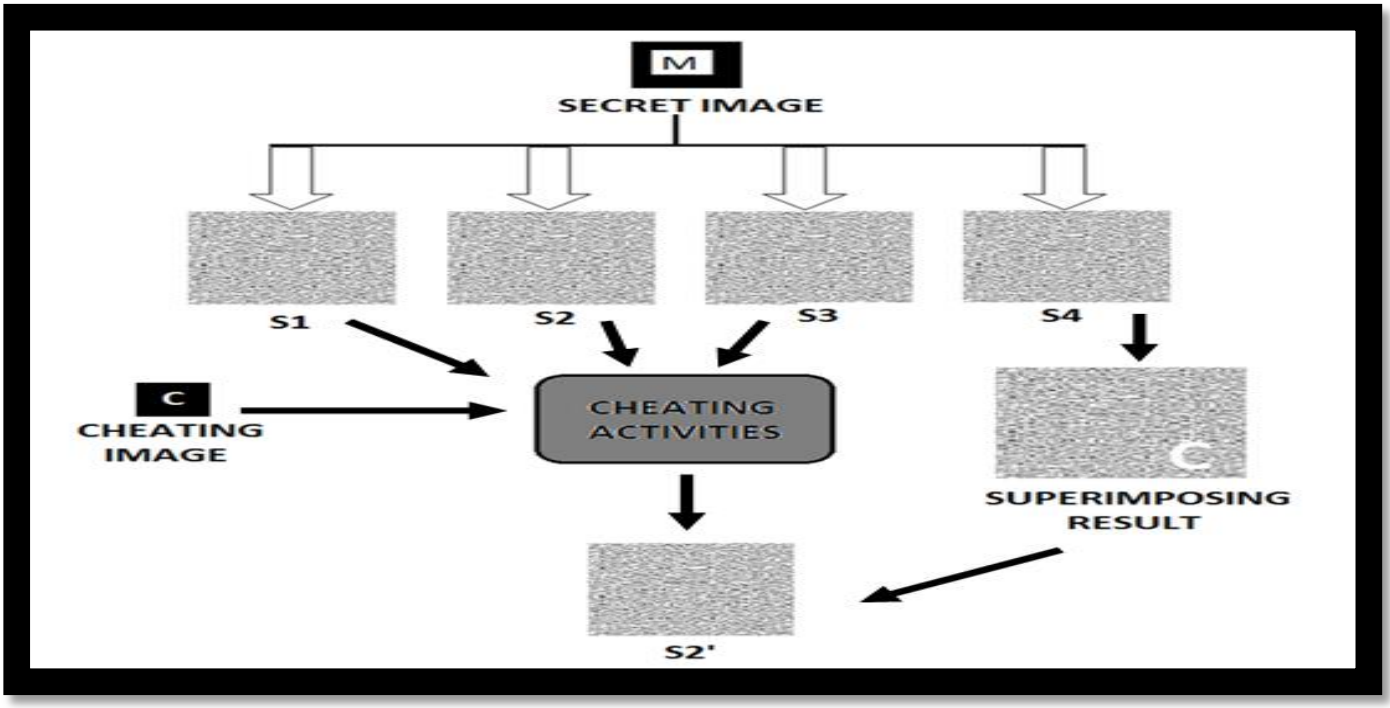

Figure 1: Recommendation Framework

II. RECOMMENDED FRAMEWORK

There are basically 2 most popular methods for achieving –Cheating Prevention Scheme which are recommended in the software and are easily used by the customers.
The two methods are :-

1) *k-out-of-n*

2) *n-out-of n*

In this paper, we use the proposed framework (Figure 1) that divides the original image into 4 shares (say) and then add a secret image to it before the users can superimpose the same.

There are two phases: learning (or training) phase and recommendation phase.

A.Training phase or Learning phase

In this phase, we construct a model which has various shares which are constructed out of original image, and with the help of any one method we put a secret image on it.

The model is used to create different shares and insert a secret image to it. The secret image is embedded into the shares so that cheating could be prevented by the cheaters.

This model consists of 5 phases-

- Chromosome creation
- Evaluation
- Selection
- Crossover
- Mutation

B.Recommendation phase

In the second phase of recommendation framework we incorporates products' maturity levels and users' receptiveness, and refine existing recommendation algorithms to take these factors into account when making a recommendation.

- *Share construction phase*

In the share construction phase, the user first generates n distinct homogeneous secret images.
Since all images can be reconstructed by other users for cheating purpose, the secret image is embedded in the same.

- *Distribution phase*

In the distribution phase, the dealer individually distributes
share s1 for x, share s2 for y, share s3 for z where s i ∈ s

III. CONCLUSION

In this paper, we propose a cheating prevention scheme using multiple secret images. It solves the cheating problem in the *k*-out-of-*n* VC without introducing extra burdens. Moreover, it is more secure than two previous proposed cheating prevention schemes. Through multiple secret images, each qualified subsets will only reveal the corresponding secret image and the other secret images are left unknown to potential cheaters. Consequently, the probability that cheaters can correctly determine the structure of victim's transparency is highly decreased. The share construction method of VC, however, cannot be directly used to deal with multiple secret images. Consequently, a new 2-outof- *n* GASCM is proposed to create shares with the same size of those in VC and the number of secret images increases from one to *(n2)*. Moreover, the performance of GASCM is improved by means of modifying initial population with filtering constraint, crossover operator with local search, and mutation operator for security. The experimental results and security analysis show that the proposed scheme does prevent victims from cheating attacks.

References

[1]A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612–613.

[2]G. Blakley, Safeguarding cryptographic keys, in Proceedings of AFIPS 1979 National Conference.

[3]M. Naor, A. Shamir, Visual cryptography, in Proceedings of advances in cryptography—EUROCRYOT'94, Lecture Notes in Computer Sciences, vol. 950, 1994. pp. 1–12.

[4]A. Shamir, M. Naor, Visual Cryptography II: Improving the Contrast via the Cover Base, Security in Communication Networks, September 16–17, 1996.

[5]C. Blundo, P. D'Arco, A. De Santis, D.R. Stinson, Contrast optimal threshold visual cryptography schemes, SIAM J. Discrete Math. 16 (2) (2003) 224–261.

[6]G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. Comput. (1996) 86–106.

[7]C. Blundo, A. De Santis, M. Naor, Visual cryptography for grey level images, Inform. Process. Lett. 75 (6) (2000) 255–259.

[8]C.C. Lin, W.H. Tsai, Visual cryptography for gray-level images by dithering techniques, Pattern Recognition Lett. 24 (1–3) (2003) 349–358.

[9]V. Rijmen, B. Preneel, ELcient colour visual encryption for shared colors of Benetton, in: Eurocrypto'96, Rump Session, Berlin, 1996.

[10]Y.C. Hou, Visual cryptography for color images, Pattern Recognition 36 (2003) 1619–1629.

[11]M. Naor, B. Pinkas, Visual authentication and identification, in: B.S. Kaliski Jr., (Ed.), Advances in Cryptology—Proceedings of Crypto 97, Lecture Notes in Computer Science, Springer, New York, vol. 1294, 1997. pp. 322–336.

[12]C.C. Chang, J.C. Chuang, An image intellectual property protection scheme for gray-level image using visual secret sharing strategy, Pattern Recognition Lett. 23 (2002) 931–941.

[13]C.C. Wang, S.C. Tai, C.S. Yu, Repeating image watermarking technique by the visual cryptography, IEICE Trans. Fundam. E83-A (2000) 1589–1598.

[14]R. Lukac, K.N. Plataniotis, Bit-level based secret sharing for image encryption, Pattern Recognition 38 (5) (2005) 767–772.

